I CLAIM:

1. A method for securing a computer system that includes one or more mobile devices and one or more a computing node, comprising:

executing a node security program in the computing node for interpreting a node security profile;

determining at least one security parameter from the interpretation of the node security profile; and

managing at least one security process between the computing node and one or more mobile devices based on the at least one security parameter determined by interpreting the node security profile.

2. The method of claim 1, wherein the at least one security process comprises a step of securing at least one of a storage area, data, file, program, process and application in at least one of the computing node, the one or more mobile devices and a resource device.

3. The method of claim 2, wherein the step of securing comprises at least one of authorizing, denying, preventing, disabling, locking and password protecting at least one of a data synchronization, data transfer, data query, data collection, network access, program execution, data manipulation. process initialization, execution and termination.

4. The method of claim 1, wherein the node security profiles comprises at least one of a text, .ini and binary, XML format.

5. The method of claim 1, wherein the at least one security parameter comprises an attribute relating to at least one of a data, file, security profile, application, process, communication and program.

6. The method of claim 1,wherein the attribute is expressed in terms of at least one of a size and type.

7. The method of claim 1, wherein the security parameter comprises at least one of a temporal or a position attribute.

8. The method of claim 1, wherein the temporal attribute is expressed in terms of at least one of a date, minute, hour, week, month and a year.

9. The method of claim 1, wherein the position attribute is expressed in terms of a position determined by at least one of a positioning technique, a zip code, an address, a region, and a location.

10. The method of claim 1, wherein the security parameter is expressed in terms of at least one of a serial number, a model number, and a software license number.

11. The method of claim 1, wherein the security parameter is expressed in terms of at least one of a mobile device type, a computing node type, a connection type, resource type and a network type.

12. The method of claim 1, wherein the network type comprises at least one of a wired and a wireless network type.

13. The method of claim 1, wherein the connection type includes at least one of a direct connection and an off-line connection between the computing node and the one or more mobile devices.

14. The method of claim 1, wherein the security parameter is expressed in terms of at least one of a physical address, a network resource ID, an IP address, a domain name, a client station ID, a mobile device ID or a server ID.

15. The method of claim 1, where the security parameter relates to handling at least one of a guest and unknown device.

16. The method of claim1, wherein the security parameter relates to managing a VPN.

17. The method of claim 1 further including transferring a device security profile to a mobile device or a resource device to be interpreted by a device security program running on the mobile device to determine device security parameters.

18. The method of claim 17, wherein transferring the device security profile comprises accessing at least one of a server station, a central station, and a computing node or a website.

19. The method of claim 17, wherein the device security profile is transferred based on at least one of a temporal attribute and a position of the mobile device in at least one of real time or non-real time modes.

20. The method of claim 17 further comprising periodically updating at least one of the node security profile and device security profile.

21. The method of claim 17, wherein the step of transferring includes at least one of a data synchronization process, data transfer, file transfer, and an email between the computing node and a mobile device ore resource.

22. The method of claim 1, wherein the step of transferring the device security profile requires at least one of a direct link and off-line link with a mobile device.

23. The method of claim1 further comprising at least one of locking and denying access to an unauthorized mobile device attempting to access the system.

24. The method of claim1 further comprising the step of locking an authorized mobile device attempting to access the network.

25. The method of claim24, wherein the locking step comprises transmitting security software to the station.

26. The method of claim 17 further including transmitting at least one of the node security profile and device security profile using at least one of a push or pull technology.

27. The method of claim 17 further including transmitting at least one of the node security profile and device security profile using an over the air protocol.

28. The method of claim 1 further including discovering at least one of one or more mobile devices and one or more resource devices.

29. The method of claim 28, wherein the at least one of one or more mobile devices and one or more resource devices are discovered remotely by running a discovery program at a central station.

30. The method of claim 28, wherein at least one of one or more mobile devices and one or more resource devices are discovered locally by running a discovery program at the computing node.

31. The method of claim 28, wherein the discovering includes detecting at least one of a device type, connection profile, location at least one of one or more mobile devices and one or more resource devices.

32. The method of claim 28, wherein the at least one of one or more mobile devices and one or more resource devices are detected based on at least one of a registry resource, a file resource, a process resource, a network management parameter, a data format, a packet format, a synchronization log entry, a directory structure or a database entry.

33. A method for managing a computer system including a computing node and one or more mobile devices, comprising:

running a discovery program to detect one or more mobile devices or resources;

determining information regarding one or more mobile devices or resources based on at least one of a registry resource, a file resource, a process resource, a network management parameter, a data format, a packet format, a synchronization log entry, a directory structure, a database entry, the presence of an executable program and attributes associated with a mobile device or resource; and

using the determined mobile device information for managing security of the computer system.

34. The method of claim 33 further including scanning the computer system based on a scan profile to detect the one or more mobile devices.

35. The method of claim 33, wherein the discovery program is run in at least one of a remote central station or a local computing node.

36. The method of claim 33 further including grouping the located mobile devices or resources by type and other attribute.

37. The method of claim 33, wherein the scan profile contains information regarding at least one of network, domain, IP address, netmask, and computer identity to be scanned, time of synchronization and device connection.

38. The method of claim 33, wherein the scan profile contains information regarding at least one of network, domain, IP address, netmask, and computer identity not to be scanned.

39. The method of claim 33, wherein the results of scanning are analyses and populated and stored and displayed to the users.

40. The method of claim 33, wherein the gather mobile device information include at least one of device type, device identity, synchronization software type, synchronization software availability, synchronization software location, synchronization software version number, previous synchronization information, data and time of last synchronization, the type of device used during previous synchronization, synchronization ID, device owner information, type of applications and files installed or used on the mobile device, file size, file name, file attribute, manufacturer information, time of all completed and incomplete synchronization and data access and connections performed, type of data and information transferred to and from a mobile device and a resource.